Einführung

Über Sanderson Forensics

Sanderson Forenscis wurde Anfang 2000 als forensische Beratungsfirma gegründet, mit dem Ziel forensische Beratungsdienste und erschwingliche, effiziente Ermittlungswerkzeuge für Strafverfolgungsbehörden anzubieten. Sanderson Forenscis verpflichtet sich, diese Werkzeuge zukünftig weiterzuentwickleln, um sicherzustellen, dass Ermittlungsbehörden Ihren Aufgaben mit den besten verfügbaren Werkzeugen zu einem günstigen Preis nachkommen können.

Systemvoraussetzungen

KaZAlyser ist entwickelt worden für Windows 98/NT/XP/ME und 2000.
Pentium III oder höher
256 MB oder mehr
minimale Bildschirmauflösung 800x600 Punkte

Haftungsauschluss

Viele Informationen, die in diesem Dokument enthalten sind, wurden im Wege des Reverse Engineering gewonnen. Man sollte sich deshalb nicht ohne Nachprüfung darauf verlassen.

KaZAlyser Überblick

KaZAlyser ist der Nachfolger des populären P2PView KaZaA/Morpheus Datenbankbetrachters. KaZAlyser stellt signifikante Verbesserungen im Ermittlungsverfahren zur Verfügung.

KaZAlyser verfügt über folgende Funktionen:

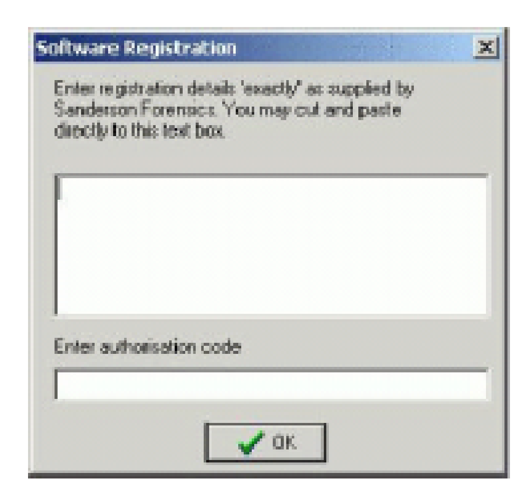
- Alle Datenbankeinträge in tabellarischer Form auflisten
- Anzeigen des Datei-Integritätsmarkers
- Erlaubt dem Ermittler jeden Datensatz zu markieren und zu kommentieren
- Identifikation von Dateien (anhand Dateiname, Schlüsselwörter etc.), bei denen es sich offensichtlich um Kinderpornografie handelt
- Identifikation von Dateien die einen bekannten Kinderpornografie-Hashwert besitzen
- Identifikation aller Grafik/Video-Dateien
- Sortierung nach beliebigen Spalten
- Datenbankexport im CSV-Format
- Entschlüsselung und Anzeige von KaZaA Media Desktop V2 Suchzeichenfolgen aus der Registrierdatenbank
- Entschlüsselung und Anzeige von Details zu entfernten Benutzern aus teilweise heruntergeladenen Dateien
- Sofern vorhanden, Entschlüsselung und Anzeige von Details zu einem entfernten Benutzer im „slackspace“ von heruntergeladenen Dateien
- Generieren von Berichten

KaZAlyser kann eine oder mehrere FastTrack-basierten Datenbankdateien, z.B. KaZaA öffnen und den Inhalt in tabellarischer Form anzeigen. Hinweis: In diesem Handbuch wird der allgemeine Begriff KazaA für alle kompatiblen Programme benutzt.
Nach dem Laden in KaZAlyser können Filter auf die Datenbankeinträge angewendet werden, um die Anzeige auf besondere Datensätze wie z.B. „alle Grafikdateien“ oder „als Kinderpornografie bekannt“ zu beschränken. KaZAlyser kann auch den Inhalt der KaZaA Registrierdatenbank anzeigen und gespeicherte Suchzeichenfolgen entschlüsseln. Die hauptsächliche Verbesserung von KaZAlyser gegenüber früheren Versionen ist seine Fähigkeit, die Quelle von heruntergeladenen Dateien zu identifizieren. KaZAlyser kann die IP-Adresse, den Benutzernamen und Datum/Uhrzeit von Teildownloads und unter gewissen Umständen von vollständigen Downloads ermitteln.

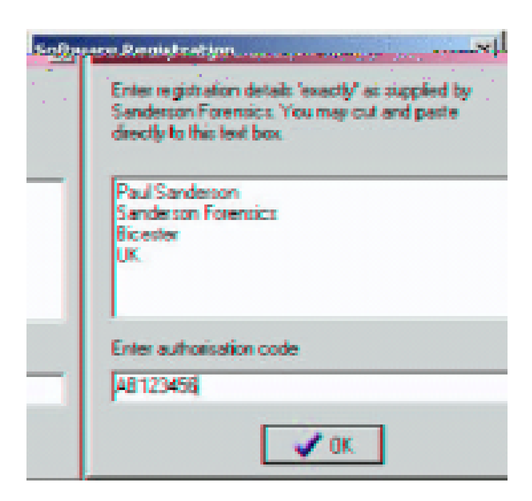
Schnellstart

KaZAlyser Registration

Wenn KaZAlyser das erste Mal gestartet wird, werden Sie aufgefordert Ihre Lizenzdaten einzugeben, die Sie beim Kauf zusammen mit dem Installationsprogramm erhalten haben.



Ihre Lizenz besteht aus bis zu 5 Textzeilen und einem Lizenzschlüssel. Geben Sie Ihre Lizenzdaten exakt so ein, wie Sie sie erhalten haben, keine zusätzlichen Leerzeichen oder andere Formatierungen, und geben Sie dann den Autorisierungscode in aus untere Feld ein.



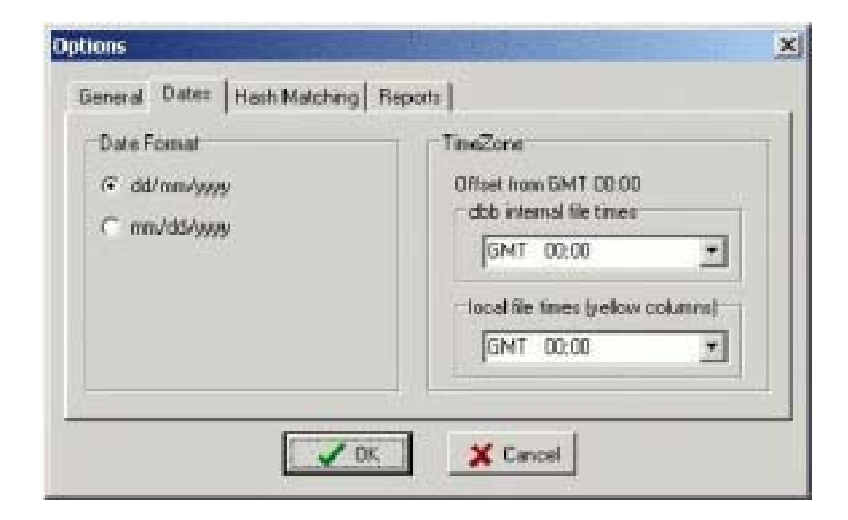
Dieser Schritt sollte nur einmal erforderlich sein.

Datumsformat-Einstellung und Zeitzonen

KaZAlyser muss konfiguriert werden, damit es mit regionalen Einstellungen Ihrer Computers übereinstimmt.

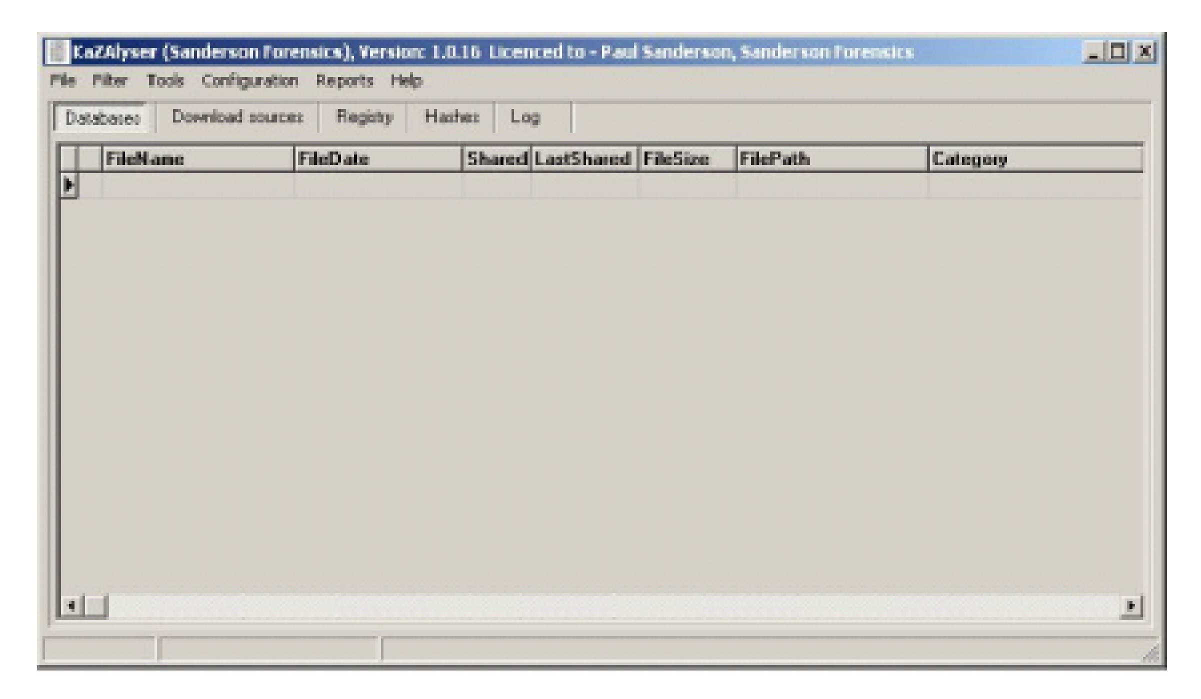
Wählen Sie das passende Datumsformat.

Für Zeitzonen zeigt KaZAlyser zwei verschiedene Datumswerte an, die durch Zeitzone und Datumsformat-Einstellungen beeinflusst werden. Der eine Wert wird aus dbb-Dateien oder Teil-Downloads, der andere aus dem Dateisystem ermittelt – im Allgemeinen das Erstellungsdatum und das Datum der letzten Änderung bzw. des Schreibvorgangs.

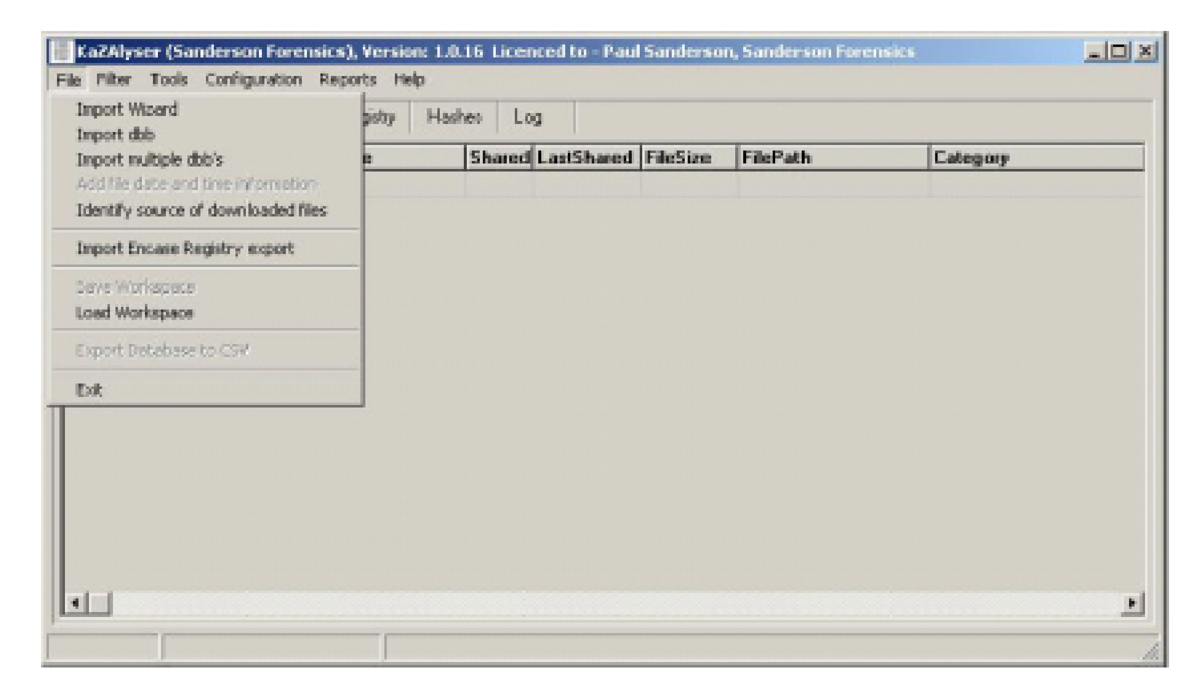


Laden und untersuchen Ihrer ersten Datenbank

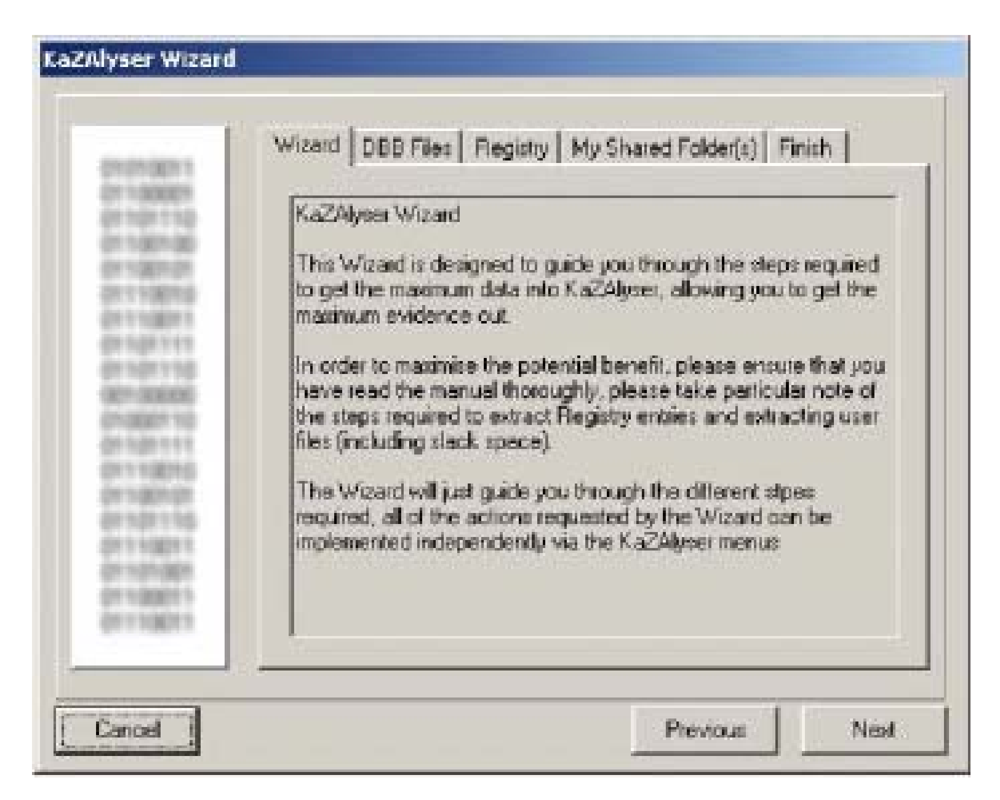
Starten Sie KaZAlyser und es wird Ihnen der folgende Bildschirm präsentiert:



Wenn der Importassistent nicht automatisch startet, wählen Sie ihn aus dem Startmenü:



Der Assistent wird Ihnen eine Reihe von Dialogfenstern anzeigen. Beachten Sie: Falls Sie einen Schritt übergangen haben oder wenn Sie mehrere Quelle laden wollen, können Sie dies im Hauptmenü erst nachholen, wenn der Assistent beendet ist.

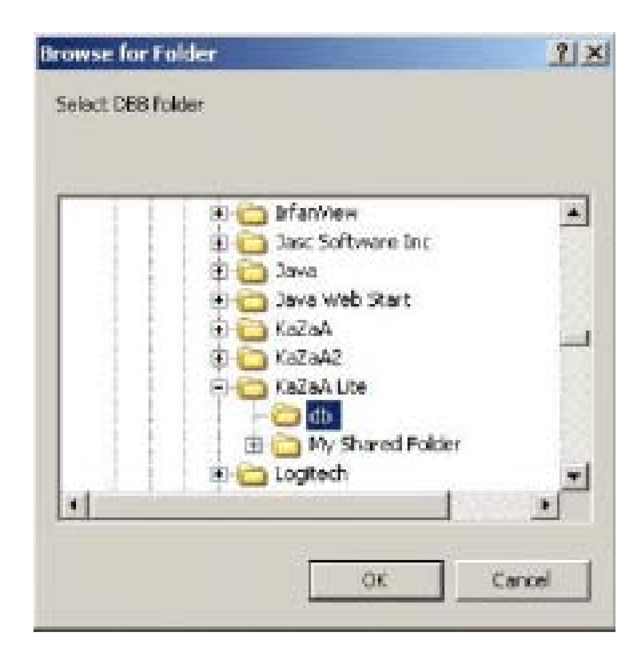


Benutzen Sie den NEXT-Button, um zur nächsten Seite zu gelangen (möglicherweise werden Sie zuvor aufgefordert Informationen einzugeben) oder benutzen Sie den PREVIOUS-Button, um zur vorherigen Seite zurückzukehren. Sie können den Assistenten jederzeit abbrechen, indem Sie den CANCEL-Button auswählen. Jeder Schritt ist optional, es können einzelne oder alle übersprungen werden.

Im ersten Dialogfenster werden Sie aufgefordert, den Ort Ihres KaZaA-Datenbankordners anzugeben.

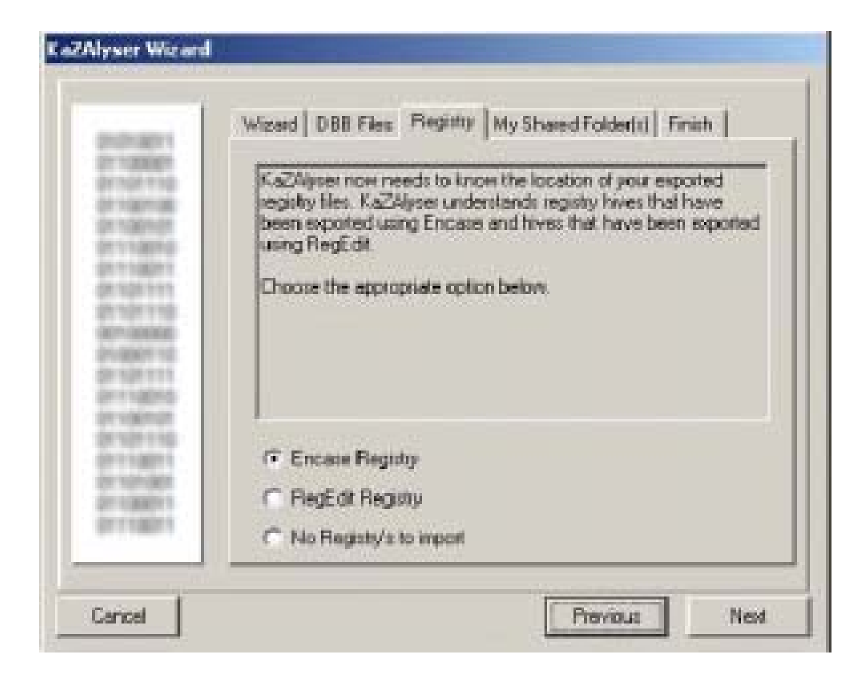


Das Drücken des NEXT-Buttons zeigt den Ordnerauswahl-Dialog an, den Sie normalerweise nutzen sollten, um den Ort eines extrahierten KaZaA-Datenbankordners auszuwählen.



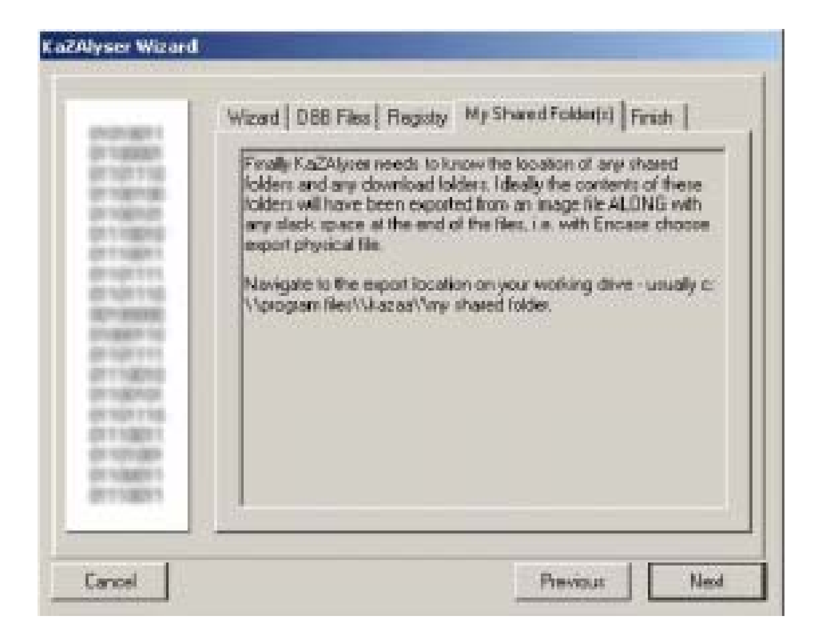
Falls Sie diesen Schritt nicht ausführen möchten, wählen Sie die Schaltfläche CANCEL.

Als Nächstes will KaZAlyser den Speicherort des KaZaA Registrierdatenbank-Extraktions-Baums wissen. Normalerweise sollte dies mit Encase extrahiert werden, wobei jeder Schlüssel als einzelne Datei vorliegt. Es ist empfehlenswert den gesamten KaZaA-Schlüssel zu extrahieren und KaZAlyser sollte auf den Root-Eintrag zeigen, d.h. {HKEY_CURRENT_USER\Software\Kazaa}.
KaZAlyser kann auch RegEdit5-Exportdaten lesen und hat RegEdit4-Exportdaten werden nur eingeschränkt untersützt:



Wählen Sie das Registrierdatenbank-Format, das Sie haben, oder „select no registry’s to import“, um diesen Schritt zu überspringen.

Der letzten Schritt besteht darin, KaZAlyser den Speicherort des gemeinsamen Ordners mitzuteilen, wenn es mehrere geben sollte (diese Information befindet sich in der Registrierdatenbank), können diese zusätzlichen Ordner später angegeben werden.



KaZaA speichert Daten, wobei laufende Downloads am Ende jeder downloadxxxxxxx.dat-Datei berücksichtigt werden. Wenn der Download beendet ist, befinden sich einige dieser Informationen manchmal im „slackspace“ am Ende dieser Datei.
In diesem Fall entschlüsselt KaZAlyser diese Informationen und zeigt sie an.

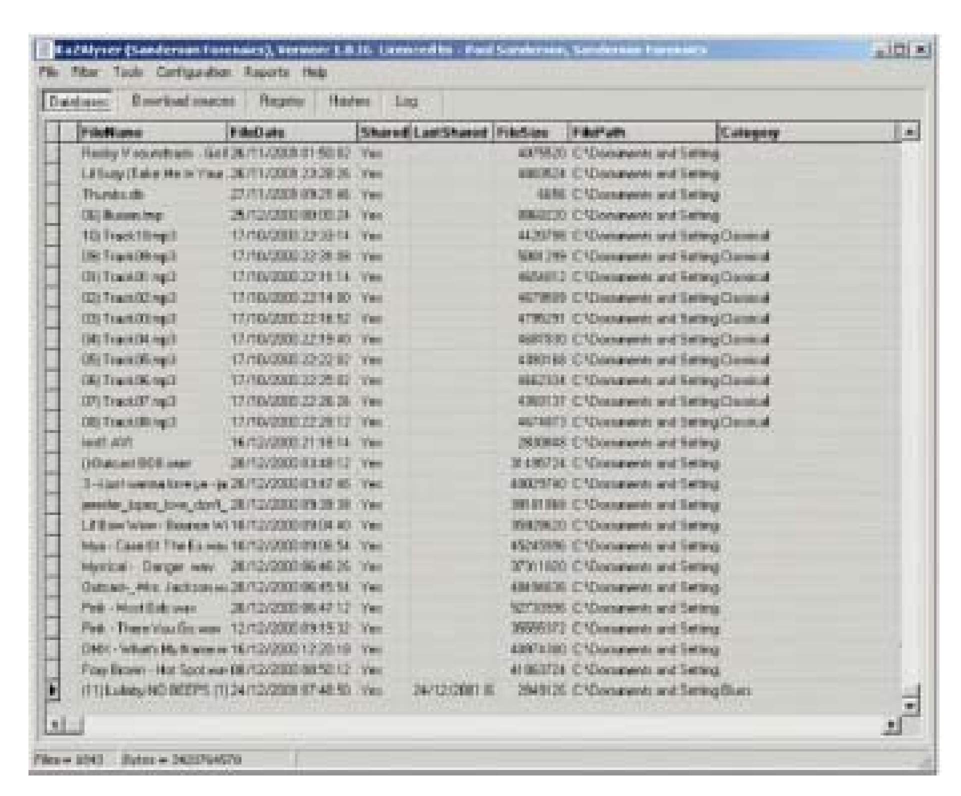
Sie sind nun in den Lage, den Befund zu überprüfen.

Navigieren und verstehen des Desktops

Die KaZaA-Daten werden im KaZAlyser in einer Reihe von Fenstern angezeigt:

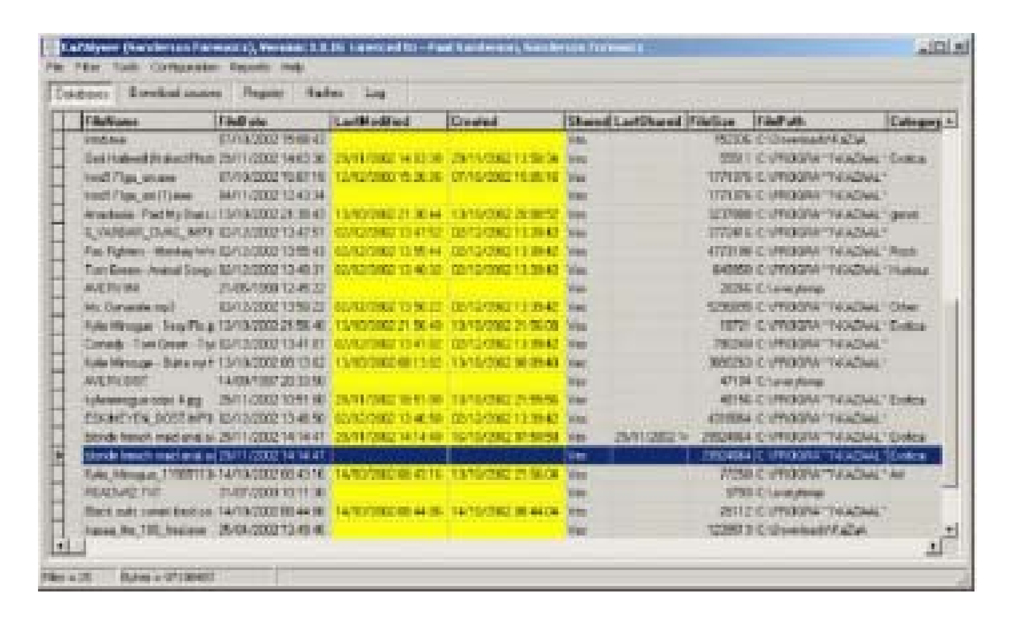
- Databases (Datenbanken)
- Download sources (Download-Quellen)
- Registry (Registrierdatenbank)
- Hashes (Hashwerte)
- Log (Logdaten)

Nach einem Klick auf „Databases“ oder „Download sources“ wird ein Bildschirm ähnlich der unten stehenden Abbildung angezeigt (vorausgesetzt, dass eine Datenbank geladen wurde):



Der Inhalt jeder dataxxx.dbb KaZaA –Datei wurde in eine Datenbank geladen und es ist/sind diese Datenbankdateien die oben abgebildet sind, oder – falls möglich – die Daten im Nachspann eines Downloads. Jede Zeile in der Datenbank entspricht einem Datensatz in der dataxxx.dbb bzw. der Download-Datei; jede Spalte in der Datenbank entspricht einem Feld innerhalb eines bestimmten Datensatzes.

Zusätzliche Datenbanken können dem Datenbankfenster entweder durch Auswahl von „Import dbb“ oder „Import multiple dbb’s“ im „File“-Menü hinzugefügt werden.

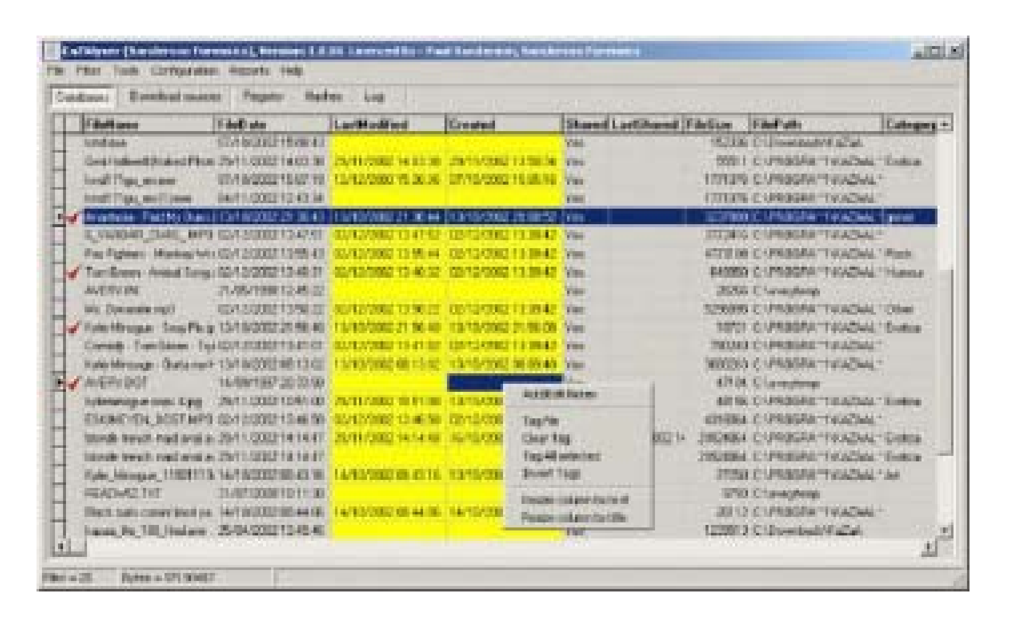


Daten, die ihren Ursprung nicht in der Datei haben, d.h. Daten, die nicht explizit innerhalb der Datei gespeichert sind, werden in einer gelb gefärbten Spalte angezeigt.

Einige Felder enthalten mehr Informationen, als sich einfach darstellen lässt. Um alle Informatioen einer bestimmten Spalte zu sehen, klicken Sie auf den rechten Spaltentrenner und ziehen die Trennlinie – dies wird die Spaltenbreite ändern. Sie können jede Spalte sortieren, indem Sie die Spaltenüberschrift anklicken. Sie können auch den Spaltenkopf auswählen und ziehen, um die Spaltenreihenfolge zu ändern.

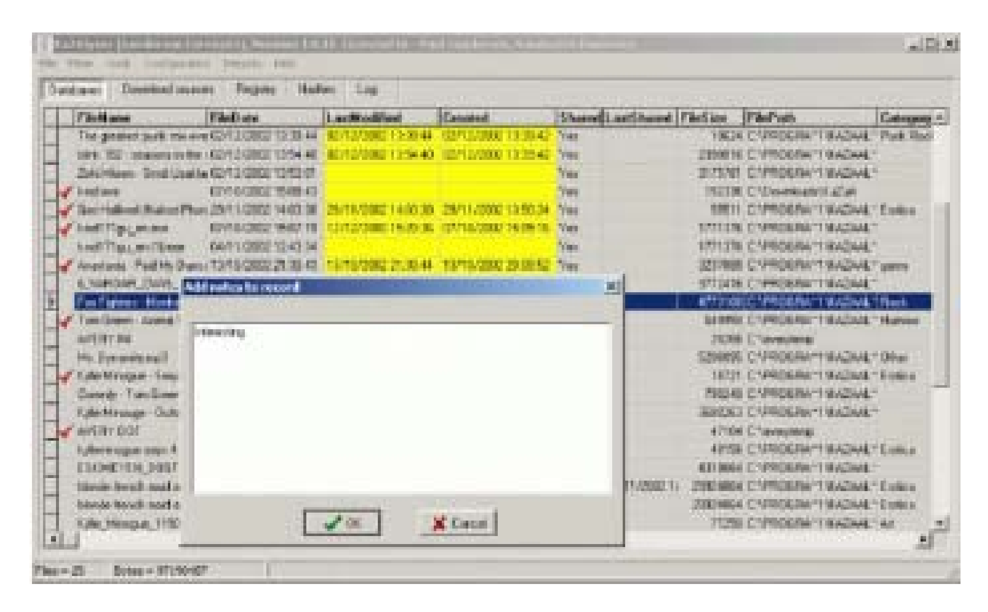
Verwenden Sie die Scrollbalken am unteren Bildschirmrand, um Spalten anzuzeigen, die nicht auf den Bildschirm passen.

Zum Hervorheben/Markieren einer Datei von Interesse drücken Sie die Leertaste oder klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie „Tag file“ aus dem Kontextmenü. Die markierte Datei wird durch eine Auswahlmarkierung am linken Rand gekennzeichnet.



Das Popup-Menü kann ebenfalls verwendet werden, alle aktuell gewählten Dateien zu markieren, die Markierungsliste umzukehren oder aufzuheben.

Sie können Bemerkungen hinzufügen/bearbeiten, indem Sie irgendwo auf dem Hauptbildschirm rechts klicken und „Add Note“ aus dem Popup-Menü wählen.



Schließlich kann das Popup-Menü auch verwendet werden, die Spaltenbreite dem breitesten Eintrag anzupassen – „Resize to text“ oder alle Spalten der Textbreite der Spaltenüberschriften anzupassen – „Resize to title“.

Filter und Berichte

KaZAlyser wird mit einem Satz von eingebauten Filtern geliefert. Diese Filter bilden auch die Basis für die Berichtsfunktionen innerhalb KaZAlyser. Ein Filter ist einfach eine Methode, um bestimmte Datensätze vor dem Anwender zu verbergen. Wenn ein Filter ausgewählte wurde, sagen wir, alle markierten Dateien, dann werden alle die Dateien nicht angezeigt, die das Markierungshäkchen nicht haben.

Es gibt zwei Hauptfilter in KaZAlyser, die einer genaueren Beschreibung bedürfen.

Wahrscheinlich Kinderpornografie (Probable child pornography)

Der Filter „Probable child pornography“ verwendet eine Datenbank mit Hashwerten bekannter Kinderpornografie; mit „bekannt“ meine ich, es ist nach der Einschätzung eines erfahrenen Polizeibeamten unwahrscheinlich, dass die Abbildungen in diesen Dateien nicht Minderjährige zeigen. Die Hashwerte wurden aus Dateien gewonnen, von denen bekannt ist, dass sie im KaZaA-Netzwerk verbreitet werden.

Bei der Datei, in der die Hashwerte gespeichert sind, handelt es sich um eine Textdatei namens „cphash.txt“, die sich im gleichen Ordner befindet, wie die exe-Datei von KaZAlyser. Die Datei enthält einfach einen 32-Zeichen-Hashwert pro Zeile. Offensichtlich ist es für einen Benutzer möglich, seine/ihre cphash.txt-Datei mit zusätzlichen Hashwerten upzudaten und deshalb ist es auch möglich, das die Datei cphash.txt Hashwerte von Dateien enthält, die nicht illegal sind. Dieses Feature sollte als Methode zum schnellen Erkennen von Dateien genutzt werden, die als Kinderpornografie bekannt sind, aber es sollte nicht als alleiniger Beweis dafür dienen, dass es sich um eine derartige Datei handelt – das heißt, der Ermittler MUSS jede Datei überprüfen, um sich zu vergewissern, dass das Material illegal ist. Außerdem sollte ein negatives Resultat dieses Filters nicht als Beweis dienen, dass sich kein illegales Material in der Datenbank befindet.

Möglicherweise Kinderpornografie (Possible child pornography)

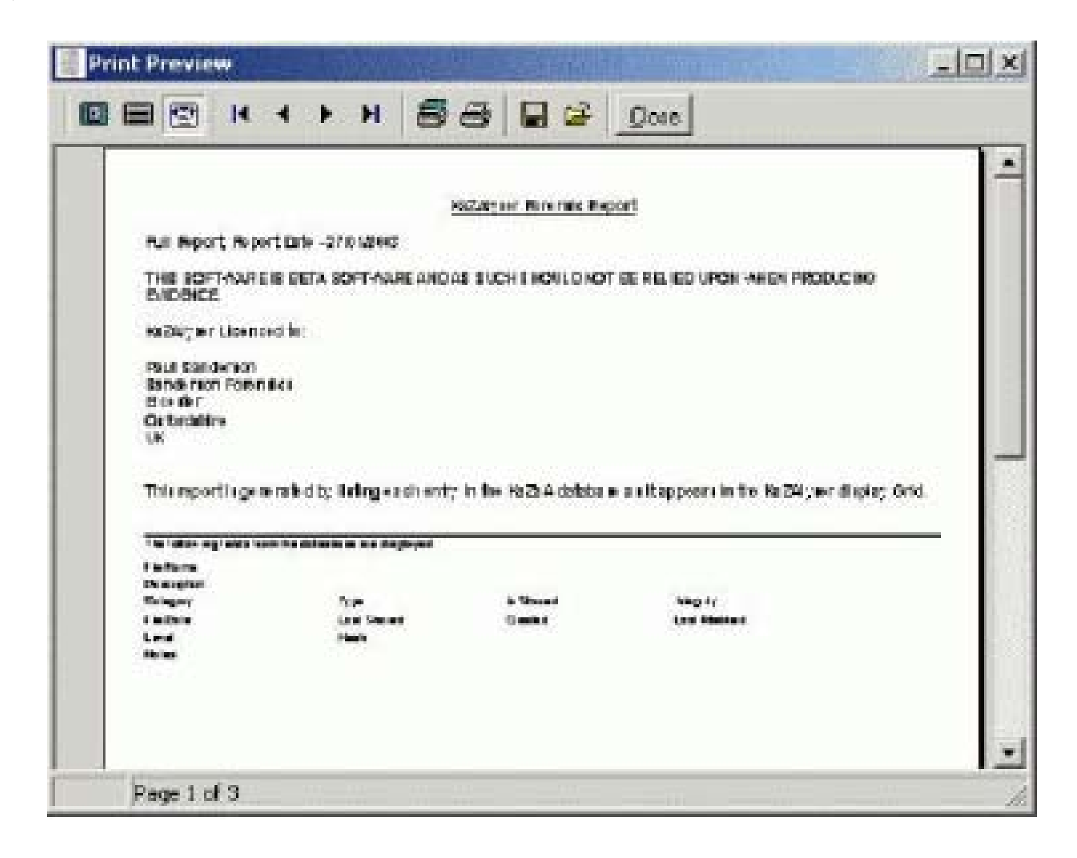
Dieser Filter arbeitet analog dem obigen in der Hinsicht, dass er Dateien basierend auf dem Inhalt einer Ursprungsdatei filtert. Die Ursprungsdatei ist in diesem Fall kp.txt, die sich ebenfalls im gleichen Ordner befindet, wie die Programmdatei. Kp.txt enthält eine Liste von Schlüsselwörtern, von denen bekannt ist, dass sie in Dateien vorkommen, die Kinderpornografie enthalten. Wenn dieser Filter anwendet wird, werden Die Felder Titel, Schlüsselwörter, Dateiname, Beschreibung und Künstler untersucht und wenn eine dieser Dateien in der KaZaA-Datenbank eines oder mehrere dieser Schlüsselwörter in der Ursprungsdatei enthält, wird der Eintrag dieser Datei hervorgehoben und anzeigt.

Es ist klar, dass die verwendeten Schlüsselwörter nicht notwendigerweise ausschließlich Kinderpornografie identifizieren und deshalb von diesem Filter erkannte Dateien möglicherweise irrtümlich als solche angezeigt werden. Es ist deshalb unbedingt notwendig, dass man dies beim Einsatz des Filters im Hinterkopf behält und alle von dem Filter identifizierten Dateien so lange mit Vorsicht genießt, bis sie unabhängig davon als illegal eingestuft sind.

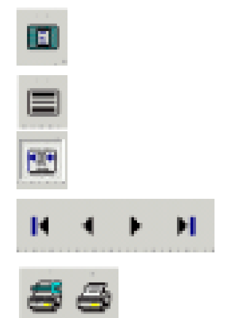
Berichte drucken

Sie könne auch verschiedene Berichte aus dem „Reports“-Menü drucken; Berichte sind im Grunde genommen Filter, deren Ausgabe an die Berichtserzeugungs-Engine weitergeleitet wird.

Jeder Bericht ist mit einer Titelseite versehen, auf die die eigentlichen Daten folgen. Der Bericht wird zunächst in einem Vorschaumodus angezeigt; der Benutzer kann ihn dann entweder speichern oder drucken.



Die Seitennavigation wird durch die Symbole am oberen Bildschirmrand ermöglicht. Diese Icons haben folgende Funktionen:



Dieses Icon erzwingt eine Berichtsvorschau im Ganzseiten-Modus, d.h., der Bericht wird in der Größe so angepasst, dass die gesamte Seite angezeigt wird

Dieses Icon zeigt den Bericht in der normalen Größe an

Verwenden Sie dieses Symbol, um die Seitenansicht auf die Bildschirmbreite anzupassen

Mit diesen Icons blättern Sie zur ersten, zur vorherigen, zur nächsten und zu letzten Seite

Verwenden Sie diese Symbole, um ihren Drucker zu konfigurieren und den Bericht zu drucken



Verwenden Sie diese Icons, um Berichte zu laden und zu speichern. Berichte können in 4 verschiedenen Formaten gespeichert werden:

Das vorgegebene und empfohlene Format ist „QuickReport file“. Dieses Format kann nur in „Quick Reports“ oder innerhalb von KaZAlyser geöffnet werden. Dieses Berichtsformat behält am besten die Text-Formatierung innerhalb des Berichts bei.

Falls Sie den Bericht in digitaler Form verteilen müssen, wählen Sie eines der anderen Formate, z.B. Text, CSV oder HTML.

Die Bedeutung der Begriffe

Datenbanken

Spalten, die in gelb angezeigt werden, repräsentieren Daten, die nicht in der dbb-Datei enthalten sind. Dies schließt Kommentare, den Namen der dbb-Datei, die Datensatznummer innerhalb der dbb-Datei und das Dateierstellungsdatum und das Änderungsdatum/die Änderungszeit ein.

Folgende Spalten sind vorhanden, sobald eine dbb-Datei geladen wurde:

FileName	Category	Type	Version	Integrity
FileDate	Title	Hash	TimeStamp	Notes
Shared	Artist	Language	Codec	DBName
LastShared	Description	Resolution	ReleaseYr	RecNo
FileSize	Keywords	Colours	Seconds	Integrity
FilePath	Album	Bitrate	OS	Notes

Obwohl den meisten dieser Spalten Daten zugeordnet sind, trifft dies nicht für alle zu. Es folgt eine Beschreibung jeder dieser Spalten, wie sie gegenwärtig verstanden werden:

Dateiname (Filename)

Dies ist der Name der Datei, wie er im KaZAlyser P2P System verwendet wird. Dies ist auch der verwendete Name der Datei, egal in welchen freigegebenen Ordnern sie sich gegenwärtig befindet.

Dateipfad (Filepath)

Dies ist der Ort auf dem verdächtigen Computer, an welchem die Datei gefunden wurde.

Dateidatum (FileDate)

Dies kann am besten beschrieben werden als letztes Datei-Speicherungs- (oder letztes Änderungs-) Datum/Uhrzeit, als die heruntergeladen oder zum ersten Mal von einem Benutzer freigegeben wurde.

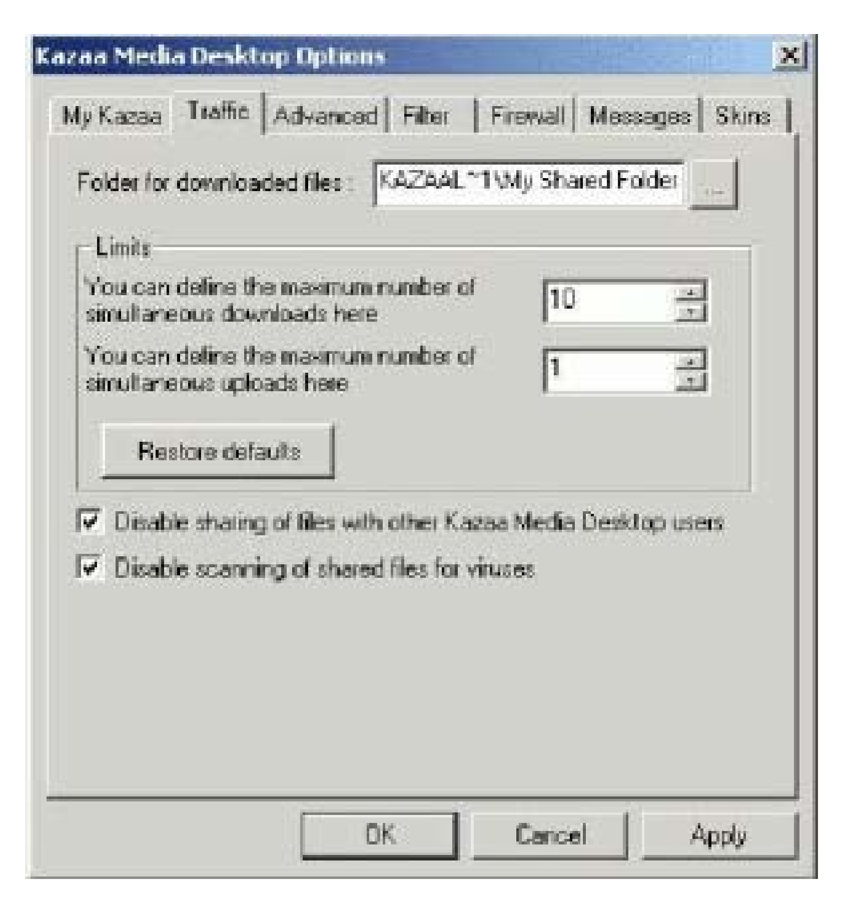
Freigegeben (Shared)

Dieses Feld zeigt an, ob eine Datei in der dbb-Datenbank als freigegeben markiert ist.

Ein KaZaA-Benutzer kann auswählen, ob eine bestimmte Datei innerhalb eines freigegebenen Ordners nicht freigegeben werden soll, indem er auf „Stop Sharing“ (vgl. nächsten Screenshot) klickt. In diesem Fall zeigt das Feld „Shared“ „No“ an.



Ein Benutzer kann das Sharing auch generell abschalten, indem er die entsprechende Option in der KaZaA Optionen (siehe nächsten Screenshot) auswählt. In diesem Fall zeigt das „Shared“-Feld weiterhin „Yes“.



Die Registrierdatenbank kann untersucht werden, um festzustellen, ob das Sharing auf Anwendungsebene abgeschaltet wurde – dies wird später noch genauer behandelt.

Zuletzt freigegeben (LastShared)

Dieses Feld wird aktualisiert, wenn KaZaA bemerkt, dass eine Datei nicht länger als freigegeben vorhanden ist, z.B. weil eine Datei, die sich einem freigegebenen Ordner befand, gelöscht oder verschoben wurde. Wenn KaZaA läuft, während die Datei gelöscht wird, dann wird das Feld üblicherweise innerhalb weniger Minuten aktualisiert. Wenn KaZaA nicht läuft, wird das Feld aktualisiert beim nächsten Start von KaZaA aktualisiert.

Dateigröße (FileSize)

Die Größe der Datei.

Kategorie (Category)

Wenn eine Datei im KaZaA P2P Netzwerk hinzugefügt wird, kann der Benutzer eine Kategorie für die Datei wählen, z.B. Rock, Humor, Erotik usw. Wenn solch ein Datei durch einen neuen Benutzer heruntergeladen wird, wird standardmäßig diese Kategorie beibehalten, aber er/sie kann sie auf Wunsch ändern.

Titel (Title)

Der Titel der Datei ist oft aussagekräftiger als der Dateiname. Er kann auch durch den Benutzer geändert werden.

Künstler, Beschreibung, Album (Artist, Description, Album)

Der Name sagt alles.

Typ (Type)

Üblicherweise beschreibt dies den Dateityp, z.B. Film, Foto, Videoclip etc.

Schlüssel (Hash)

Dies ist ein 20 Byte großer Hashwert, der aus einer 16 Byte MD5 Prüfsumme und einer 4 Byte großen CRC-Prüfsumme (Cyclic Redundancy Code) besteht. Der MD5-Teil des Hashwertes wird aus den ersten 300 KB der Datei berechnet. Der Algorithmus der verbleibenden 4 Byte CRC-Prüfsumme konnte bis jetzt nicht vollständig identifiziert werden.

Sprache (Language)

Die Sprache der Datei, sie kann durch den Benutzer angegeben oder geändert werden.

Erscheinungsjahr, Version, Betriebssystem (ReleaseYr, Version, OS)

Ebenfalls benutzerdefiniert.

Auflösung, Farben, Bitrate, Codec, Sekunden (Resolution, Colours, Bitrate, Codecs, Seconds)

Diese Angaben werden durch KaZaA ermittelt und dargestellt.

Zeitstempel (TimeStamp)

Dieses Feld hat üblicherweise keinen Inhalt und sein Zweck ist bisher unbekannt.

Integrität (Integrity)

Das Integrity-Feld ist neu in KaZaA Media Desktop V2 oder höher und ist eine Methode über die KaZaA seine Benutzer bewertet. Ein Benutzer wird ermuntert eine Datei zu bewerten (schlecht, gut oder exzellent). Wenn solch eine Datei später von einem Benutzer heruntergeladen wird, erhöht sich sein oder ihr Bewertungsstatus im KaZaA Netzwerk.

Wichtig aus Strafverfolgungssicht ist, dass eine durch Benutzer „A“ bewertete, aber durch Benutzer „B“ heruntergeladene Datei, keinen Bewertungsstatus aufweist. Ist also eine Integritätsbewertung gesetzt, dann handelt es sich bei dem Benutzer der untersuchten KaZaA-Installation um denjenigen, der diese Bewertung abgegeben hat – dies beweist im Beispiel das Wissen von Benutzer „A“ über die Dateiexistenz.

Datenbankname (DBName)

Der Dateiname und –pfad der dbb-Datenbank-Datei aus welcher der Datensatz extrahiert wurde.

Datensatznummer (RecNo)

Die Datensatznummer innerhalb der o.g. Datenbank.

Kommentare (Notes)

Dies sind Anmerkungen, die durch den Ermittler angefügt wurden.

Downloadquelle (Download source)

Die Seite „Downloadquellen“ zeigt folgende Felder an:

CRC	LastModified	Keywords	Codec
FileName	Hash	Resolution	Integrity
Sources	RemoteName	Category	releaseYr
State	Size	OS	LocalPath
RemoteIP	SuperNodeIP	Colours	StartTime
UserStatsUpdat	Title	Type	Notes
ed	Seconds	Bitrate	RecNo
UserID	Artist	Version	
FileNameDate	Album	TimeStamp	
Created	Language	Description	

Jedes dieser Felder wird nachfolgend besprochen.

CRC-Prüfsumme (Cyclic Redundancy Code)

Wenn ein gewähltes Verzeichnis nach Downloadquellen untersucht wird, unternimmt KaZAlyser folgende Schritte für jede Datei:

1. sucht nach einem Vorspann in der aktuellen Datei
2. berechnet die CRC-Prüfsumme für den Trailer neu und vergleicht sie mit der CRC-Prüfsumme innerhalb des Vorspanns
3. Berechnet einen Schlüsselwert für den eigentlichen Dateiinhalt und überprüft, ob der neu berechnete Schlüsselwert mit dem Schlüsselwert übereinstimmt, der im Vorspann gespeichert ist.

Wenn die Schritte 2 und 3 erfolgreich sind, protokolliert KaZAlyser in der CRC-Spalte „verified“ (=überprüft), d.h., KaZAlyser stellt sicher, dass die vorgefundenen Daten zu der aktuellen Datei gehören und überprüft, dass sie nicht beschädigt sind. Wenn die CRC-Prüfsumme nicht übereinstimmt, versucht KaZAlyser trotzdem, die Daten des Vorspanns sinnvoll zu interpretieren.

Wenn der Schlüsselwert nicht mit der zugeordneten Datei übereinstimmt, wird kein Eintrag in den Downloadquellen angezeigt.

Dateiname (FileName)

Dabei handelt es sich um den Pfad und den Namen der Datei im lokalen Dateisystem.

Quellen (Sources)

KaZaA unterstützt „swarming downloads“, d.h., eine Datei kann aus mehreren Quellen zur gleichen Zeit heruntergeladen werden. Dieses Feld zeigt die Zahl der Quellen an, von denen die Dateien heruntergeladen wurden. Wird im Feld eine „4“ angezeigt, sehen Sie 4 Datenzeilen im KaZAlyser-Fenster, eine für jede Downloadquelle.

Status (State)

Der Download-Status – im Gange oder pausierend

Ferne IP-Adresse (RemoteIP)

Die IP-Adresse des Computers, von dem diese Datei heruntergeladen wurde, dies kann eine von mehreren Quellen sein.

Es gibt verschiedene Datums- und Zeitangaben, die zu diesem Download gehören. Es sollten alle untersucht werden um festzustellen, ob es sich um eine verlässliche IP-Adresse handelt.

Benutzerstatus aktualisiert (UserStatsUpdated)

Dieses Feld scheint in unregelmäßigen Intervall aktualisiert zu werden, manchmal überhaupt nicht. Wenn ein Eintrag vorhanden ist, kann mit Sicherheit gesagt werden, dass die RemoteIP zu diesem Zeitpunkt benutzt wurde.

Datum des Dateinamens (FileNameDate)

Ein Feldinhalt ist nur bei teilweisen Downloads vorhanden, wenn die Dateinamen die Form „downloadxxxxxxxxxxxxxxxxxx.dat“ haben, wobei die „x“ Zahlen repräsentieren. Die ersten 10 enthalten codiert Datum und Uhrzeit. Dies kann der Zeitpunkt sein, an dem der Download gestartet wurde, d.h., als der Benutzer die Datei angefordert hat. Dieses Datum ist normalerweise jünger als das Dateisystemdatum.

Erstellt (Created)

Datum und Uhrzeit, als diese Datei auf dem untersuchten Computer erstellt wurde – diese Zeit ist direkt aus dem Dateisystem ermittelt, nicht aus der heruntergeladenen Datei. Es handelt sich um die tatsächliche Startzeit des Downloads oder bei einem teilweisen Download um die Endezeit des letzten Downloadsegments.

Zuletzt geändert (LastModified)

Zeitpunkt, an dem die Datei zuletzt geändert/gespeichert wurde. Dies ist das tatsächliche Ende des Downloads.

Startzeit (StartTime)

Dieser Zeitpunkt liegt normalerweise vor dem „FileNameDate“ und könnte Datum/Uhrzeit angeben, an dem KaZaA gestartet wurde.

Schlüsselwert (Hash)

Der Schlüsselwert der Datei. Dies ist der Schlüsselwert eines vollständigen Downloads, oder der Schlüsselwert, den eine Datei hat, wenn der Download für „partial downloads“ komplett ist.

Benutzer-ID (UserID)

Die Benutzer-ID des Benutzers, von dem die Datei heruntergeladen wurde. BenuterIDs sind in KaZaA nicht eindeutig.

Größe (Size)

Die Größe, die der Download haben wird, wenn die Datei vollständig heruntergeladen ist.

IP des Superknoten (SuperNodeIP)
Die IP-Adresse des Superknoten, der die Verbindung zwischen dem Benutzer und dem entfernten Computer ermöglicht.

Title, Seconds, Artist, Album, Language, Keywords, Resolution, Category, OS, Colours, Type, Bitrate, Version, TimeStamp, Description, Codec, Integrity, ReleaseYr, Size

All diese Felder werden im Abschnitt Datenbank weiter oben beschrieben.

Die Registrierdatenbank verstehen

KaZAlyser zeigt die Registrierdatenbank auf zwei Arten an, RAW bedeutet Anzeige aller Registrierdatenbank-Einträge ungeachtet ihres kriminaltechnischen Beweiswerts. PROCESSED (= aufbereitet) zeigt die wahrscheinlich nützlichsten Registrierdatenbank-Einträge. Die Daten des aufbereiteten Registrierdatenbank-Fensters werden in den KaZAlyser-Bericht importiert.

Vermutlich die nützlichste Information in der KaZaA-Registrierdatenbank sind die zuletzt verwendeten Suchbegriffe. Diese Information wird nur in KaZaA Media Desktop Version 2 und höher gespeichert, wobei die letzten 50 Suchbegriffe aufgezeichnet und in verschlüsselter Form gespeichert werden.

KaZAlyser dekodiert die Sucheinträge der Registrierdatenbank und zeigt sie im Registrierdatenbank-Fenster an.

Weitere nützliche Registrierdatenbank-Einträge sind:

- Der Ort freigegebender Ordner
- Der Benutzername
- E-Mail-Adresse
- Länderkennung
- Die Downloadbandbreite
- Die Zahl gleichzeitiger Downloads und Uploads
- Ob „gemeinsame Nutzung“ eingeschaltet ist

Nicht alle der genannten Informationen sind vorhanden und nicht alle sind verlässlich.

Schlüsselwerte (Hashes)

KaZaA verwendet beim Aufzeichnen von Dateien und gleichzeitigen Downloads Schlüsselwerte. Der Schlüsselwert ist 20 Byte groß und besteht aus einer 16 Byte MD5-Signatur, die auf den ersten 300 KB der Datei basiert, und einer 4 Byte umfassenden zweiten Checksumme (CRC).

KaZAlyser wird mit einer kleinen Hash-Bibliothek bekannt gewordener Kinderpornografie ausgeliefert. Sollten Sie diese Bibliothek erweitern wollen, können Sie Ihre eigenen KaZaA-Hashes über ein der Optionen aus dem Tools-Menü erstellen.

Beachten Sie, dass die von KaZAlyser erzeugten Schlüsselwerte nur MD5-Hashes sind und nicht die zusätzliche 4-Byte CRC enthalten. Deswegen ist es möglich, dass – obwohl KaZAlyser Dateien mit übereinstimmenden Hashes identifizeren kann – zwei Dateien einen identischen Schlüsselwert aufweisen. Dies passiert z.B., wenn zwei Film-Dateien existieren und einer davon ist länger als der andere, aber beide stimmen in den ersten 300K überein. Sie MÜSSEN überprüfen, dass eine durch KaZAlyser identifizierte Datei tatsächlich die ist, die Sie meinen.Obwohl ich erlebt habe, dass KaZAlyser zwei unterschiedlich lange Dateien mit dem gleichen Hash identifiziert hat, wurden sie immer korrekt als Kinderpornografie identifziert, z.B. unterschiedliche Versionen derselben Datei.

Die Log-Datei

Zeigt grundlegende Log-Informationen über die von KaZAlyser unternommenen Prozesse.

Grundlagen

KaZaA zusätzliche Datenbanken hinzufügen

Sobald der Import-Assistent gelaufen ist, oder anstatt den Assistenten zu benutzen, kann zusätzlich eine Datenbank für gleichzeitige Ermittlungen geladen werden.

Wählen Sie File|Import dbb oder File|Import multiple dbb's aus dem Menü. Wenn Sie eine einzelne dbb-Datei laden, werden Sie aufgefordert, die Datenbank auszuwählen, die Sie untersuchen wollen, wenn Sie mehr als eine Datenbank laden, werden Sie aufgefordert, den Ordner auszuwählen und alle *.dbb-Dateien in dem ausgewählten Ordner werden zur Untersuchung geöffnet.

Dateidatum und -zeit-Informationen hinzufügen

Das Hinzufügen weiterer Datums- und Zeit-Informationen für eine physische Datei, die mit einem Datensatz in der dbb-Datenbank korrespondiert, stellt sich wie folgt dar:

1. Identifizieren Sie den freigegebenen Ordner, der der aktuell in KaZAlyser geladenen dbb-Datenbank zugeordnet ist
2. Wählen Sie „Add file date and time information“ aus dem Datei-Menü
3. Navigieren Sie mit Hilfe des „Browse For Folder“-Dialogs zu dem in Schritt 1 identifizierten Ordner

KaZAlyser wird nun:

a. Der Reihe nach jede Datei im freigegebenen Ordner öffnen und einen Schlüsselwert berechnen
b. Den berechneten Hashwert und diesen mit den Dateien in der geladenen dbb-Datenbank vergleichen, um festzustellen, ob einen Übereinstimmung gefunden wurde
c. Die Informationen „Date Last Written“ und „Date Created“ direkt aus der Datei ermitteln und diese bei dem passenden Datensatz anzeigen

Diese Information wird nun in einer gelben Spalte angezeigt und kann verwendet werden, um zu versuchen zu ermitteln, ob eine Datei aus dem Internet geladen oder durch einen Benutzer in den freigegebenen Ordner kopiert wurde.

Die Quelle eines Downloads identifizieren

Teilweise heruntergeladenene Dateien

Wenn eine Datei von KazaA heruntergeladen wird, geschieht das in Blöcken und jeder Block wird in einer temporären Datei mit einem Namen wie „download112003400102.dat“ gespeichert. Diese Datei beginnt mit den Daten der Datei, die gedownloaded werden soll und endet mit einem Nachspann, der Daten in Bezug auf die Quelle enthält, darunter den Benutzernamen der Person, von der die Datei heruntergeladen wurde und die letzte IP-Adresse dieses Benutzers. Dieser Nachspann enthält auch den Datei-Hashwert.

Falls die Datei von unterschiedlichen Orten heruntergeladen wurde, gibt es für jeden entfernten Benutzer einen Eintrag.

Um die teilweisen Downloads zu laden und anzuzeigen, wählen Sie den Menüeintrag „File|Identify source of downloaded files“. Wählen Sie den Speicherort der teilweise heruntergeladenen Dateien (normalerweise „my shared folder“) und klicken Sie auf das „Partial Download“-Register im oberen Bereich von KaZAlyser, um die Ergebnisse zu sehen.

KaZAlyser tut folgendes:

1. sucht nach einem Nachspann in jeder Datei im gewählten Ordner
2. berechnet eine neue CRC für den Nachspann und vergleicht sich mit der CRC, die im Nachspann gespeichert ist
3. berechnet einen neuen Hashwert für den Dateiinhalt und stellt sicher, dass der neue Hashwert mit dem Hashwert im Nachspann übereinstimmt
4. falls beides übereinstimmt, werden die Details in die KaZAlyser-Tabelle übernommen

Vollständig heruntergeladene Dateien

Offensichtlich sind die Daten in der dbb-Datei nur Teil der Geschichte, falls die freigegebenen Dateien auch auf dem System vorhanden sind, können weitere Informationen aus ihnen gewonnen werden. Sobald eine KaZaA-Datenbank in KaZAlyser geladen wurde, können die zugehörigen Datums- und Zeitangaben aus der eigentlichen Datei zur Anzeige hinzugefügt werden. Um dies tun zu können, müssen die Dateien selbst auf dem untersuchten System vorhanden sein und müssen aus dem Image in einer Weise extrahiert worden sein, die Datums- und Zeitstempel beibehält.

In Encase navigieren Sie z.B. zu „My Shared Folder“ oder einem anderen relevanten Ordner, führen einen Rechtsklick auf dem Ordner aus und kopieren die Dateien aus dem Image – stellen Sie sicher, dass Sie die physische Datei extrahieren, d.h. alle Bytes in der Datei einschließlich des sog. „slack space“ des letzten Clusters. Wählen Sie dann „File|Load Files“ in KaZAlyser; auf jede Datei in dem gewählten Ordner wird zugegriffen und ein Hashwert berechnet, wenn eine Datei mit einem passenden Hashwert in der Datenbank vorhanden ist, dann werden für jede passende Datei das letzte Speicher- und das Erstellungsdatum der Datenbank hinzugefügt und auf dem Bildschirm angezeigt.

Diese Information kann zur Widerlegung von Einwänden nützlich sein, wie z.B. „die Dateien wurden alle in einem Rutsch von einem einzelnen Benutzer heruntergeladen“.

Bei vollständig heruntergeladenen Dateien macht KaZAlyser folgendes:

1. sucht nach einem Nachspann im „slack space“ jeder Datei des ausgewählten Ordners
2. berechnet eine neue CRC für den Nachspann und vergleicht sie mit der CRC, die im Nachspann gespeichert ist
3. berechnet einen neuen Hashwert für den Dateiinhalt und stellt sicher, dass der neue Hashwert mit dem Hashwert im Nachspann übereinstimmt
4. Falls sie nicht übereinstimmen, versucht KaZAlyser die Benutzerdaten aus dem teilweisen Nachspann-Datensatz zu extrahieren

Das Laden der Registrierdatenbank

Um die Registrierdatenbank-Einträge einer KaZaA-Installation untersuchen zu können, müssen die Schlüssel der Registrierdatenbank zunächst in einer Form extrahiert werden, mit der KaZAlyser etwas anfangen kann. KaZAlyser versteht drei verschiedene Registryformate: RegEdit 4-Exporte, RegEdit 5-Exporte und Encase Exporte.

Encase Registry Exporte

In Encase navigieren Sie zu dem relevanten Registry-Zweig und wählen „File Structure" aus dem Popup-Menü. Nachdem Encase die Registry geladen und die Struktur entschlüsselt hat, navigieren Sie zu dem KaZaA-Registryschlüssel – normalerweise [HKEY_CURRENT_USER\Software\Kazaa] obwohl dies in der Encase-Registry „NTUSER.DAT\NTRegistry\$$$PROTO.HIV\Software\Kazaa" entspricht – klicken Sie rechts auf den Ordnernamen und wählen Sie „copy folders". Für weitere Informationen ziehen Sie das Encase-Benutzerhandbuch zu Rate.

Nachdem die Registry-Schlüssel mittels Encase extrahiert wurden, müssen wir sie in KaZAlyser importieren. Wählen Sie „File|Import Encase registry export" aus dem Menü und navigieren Sie zu dem Ordner, in dem sich die zuvor extrahierten Registry-Einträge befinden.

KaZAlyser wird alle Registry-Schlüssel laden und anzeigen. Verschlüsselte Werte – z.B. die Suchschlüssel – werden entschlüsselt und im Klartext angezeigt.

Regedit Exporte

Extrahieren Sie mit Hilfe eines geeigneten Werkzeugs die Registry-Datei und navigieren Sie zu dem gewünschten Schlüssel, exportieren Sie den Registry-Schlüssel und die Unterschlüssel entweder im Version 4 oder Version 5 kompatiblen Format. Importieren Sie die resultierende Datei in KaZAlyser über den Menüpunkt „File|Import registry keys".

Hashwerte

KaZAlyser wird mit einen kleinen Bibliothek bekannter Kinderpornografie-Hashwert ausgeliefert.

Um diese Bibliothek zu erweitern, stellt KaZAlyser drei Hash-Funktionen zur Verfügung:

Generate hash on single file

Diese Option erzeugt einen einzelen KaZaA-MD5-Hashwert aus den ersten 300 KB der ausgewählten Datei.; der Hashwert wird in der Textbox unter dem „Hashes“-Register angezeigt.

Generate hash on contents of folder

Diese Option erzeugt den KaZaA-Hashwert für alle Dateien des ausgewählten Ordners.

Generate hash on contents of tree

Diese Option erzeugt den KaZaA-Hashwert für alle Dateien des ausgewählten Ordners und alle seine Unterordner.

Nachdem Sie einen oder mehrere Hashwerte erzeugt haben, können diese aus der Hash-Anzeige kopiert und die Datei cphash.txt eingefügt werden. ***Bitte beachten Sie: KaZAlyser Fähigkeit Dateien mit kinderpornografischem Inhalt über seine Hash-Engine zu erkennen, ist nur so gut wie der Inhalt der Datei cphash.txt. Lassen Sie große Sorgfalt walten, um eine „Verseuchung“ zu vermeiden.***

Das Speichern Ihrer Arbeit und das Laden einer gespeicherter Arbeitssitzung

Wählen Sie „File|Save Workspace“ aus dem Menü und dann einen geeigneten Ort für Ihre aktuelle Arbeitssitzung. Alle aktuellen Einstellungen (Marken, Kommentare etc.) bleiben erhalten.

Zu einem späteren Zeitpunkt wählen „File|Load Workspace“, um einen vorherigen Fall zu laden.

KaZAlyser konfigurieren

Konfigurieren Sie die KaZAlyser-Laufzeit-Optionen über den „options“-Dialog. Wählen Sie „Tools|Options“ aus dem Menü. Auf der ersten Options-Registerseite geht es um allgemeine Programmeinstellungen:

General



Case sensitive sorting

Wenn ausgewählt, wird eine Großbuchstabe wie ein Kleinbuchstabe behandelt, „A“ ist sozusagen dasselbe wie „a“. Wenn nicht ausgewählt, gilt die Reihefolge a, b, c, d,.....z, A, B, C etc.

Remember last directories

Falls ausgewählt, merkt sich KaZAlyser die zuletzt benutzten Verzeichnisse/Ordner und verwendet sie als Startpunkt für zukünftige Dateioperationen.

Run wizard at startup

Entfernen Sie das Häkchen um zu verhindern, dass der Assistent beim Aufruf von KaZAlyser gestartet wird.

Write debug log

Falls ausgewählt, schreibt KaZAlyser automatisch eine ausführliche Logdatei im Programmordner (z.B. \Programme\Sanderson forensics\KaZAlyser\debug.log). Verwenden Sie diese Auswahl, wenn Sie Probleme haben und Debug-Informationen an Sanderson Forensics senden möchten. Debug-Logdaten werden bei jedem Programmlauf angehängt, so dass die Datei sehr groß werden kann. Bitte stellen Sie sicher, dass diese Option nur eingeschaltet ist, wenn sie benötigt wird.

Force CRC check on downloads

Falls “Identify download sources” ausgewählt ist, kann KaZAlyser überprüfen, ob die CRC den Nachspanns mit den verknüpften Daten korrespondiert. Bei eingeschalteter Option ist die Fehlerprüfung von Encase genauer und kann dazu führen, dasss KaZAlyser mögliches Beweismaterial übersieht. Ein Ausschalten der Option kann zu einem Absturz von KaZAlyser führen. Wählen Sie die Option, wenn KaZAlyser abgestürzt ist oder andere Probleme während der Aktion „Identify download sources“ aufgetreten sind.

Dates



In diesem Dialog geht es darum, wie Datumswerte angezeigt und in KaZAlyser interpretiert werden.

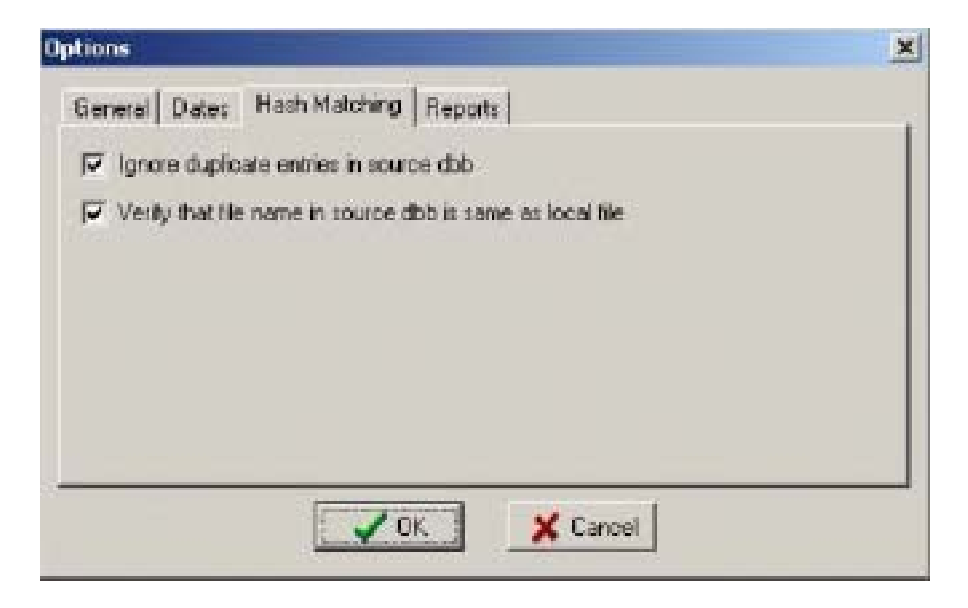
Date Format

Zur Zeit verwendet KaZAlyser nur amerikanische und englische Datumsformate.

TimeZone

Sie können zwei Zeitzonen wählen. Die Zeitverschiebung wird sowohl auf Datums- und Zeitwerte angewendet, die in der KaZaA-Datenbank gespeichert sind als auch auf Datums- und Zeitwerte in freigegebenen Ordnern.

Hash Matching



Verwenden Sie diese Einstellungen um festzulegen, wie mit Dateien in „Gemeinsame Dateien“ (und anderen Ordnern) verfahren wird, beim Versuch, sie gegen Dateien in einer dbb-Datenbank abzugleichen. Diese Option kontrolliert, wie eine Dateienvergleich durchgeführt wird, wenn „Add file date and time option“ verwendet wird.

Ignore duplicate entries in source dbb

Falls ausgewählt, stoppt KaZAlyser die Vergleichssuche für die aktuelle Datei bei der ersten Hashwert-Übereinstimmung in der Datenbank.

Verify that file name in source dbb is same as local file

Wenn diese Option gewählt ist, wird eine Datei nur dann angezeigt, wenn sowohl Hashwert als auch Dateiname übereinstimmen.

Reports



Diese Optionen legen fest, wie KaZAlyser Berichte anzeigt.

Display descriptions

Wählen Sie dies, damit KaZAlyser eine Inhaltsbeschreibung auf der Titelseite des Berichts anzeigt.

Start body of report on page 2

Wenn diese Option gewählt ist, beginnen die eigentlichen Berichtsdaten auf der zweiten Seite, ansonsten direkt nach der Einleitung auf der ersten Seite.

Display abbreviated registry entries

Wenn aktiviert, werden die Registry-Einträge des “Processed registry”-Fensters ausgegeben, ansonsten erscheint eine vollständige Auflistung aller Registry-Einträge („raw registry“) im Bericht.

Wie KaZaA Daten speichert

KaZaA speichert nützliche Informationen hauptsächlich an drei Stellen:

Dbb-Dateien

Dbb-Dateien sind die Methode, mit der KaZaA verfolgt, welche Dateien aktuell freigegeben sind; die dbb-Datei finden Sie normalerweise im Unterordner \db des KaZaA-Installationsverzeichnisses. Die dbb-Datei ist im Grunde genommen eine Datenbank freigegebener Dateien.

Wenn ein Benutzer einen Ordner zur Freigabe auswählt, legt KaZaA einen Eintrag in der dbb-Datenbank für jede Datei in diesem Ordner an. Bestimmte, von KaZaA erzeugte Informationen werden ebenfalls für jede Datei gespeichert. Dies beinhaltet einen Hashwert, der über verschiedene Teile der freigegebenen Dateien generiert werden, die Farbtiefe eines Bildes, die Länge eines Filmes usw.

Der Benutzer kann auch selbst zusätzliche Informationen in der Datenbank ablegen, z.B. Schüsselwörter oder eine Beschreibung der Datei und den Künstler und das Album einer Musikdatei.

Wenn eine Datei aus dem KaZaA-Netzwerk heruntergeladen wird, wird es standardmäßig im Ordner „Gemeinsame Dateien“ („my shared folders“) abgelegt und **automatisch** im KaZaA-Netzwerk freigegeben. Die gesamte von einem Benutzer hinzufügte Information ist in diesem Fall diejenige, die aus der heruntergeladenen Datei bezogen wurde. Sie erbt sozusagen die Benutzerinformation der heruntergeladenen Site.

Falls sich der Benutzer entscheidet, eine bestimmte Datei nicht freizugeben (indem er in KaZaA rechts klickt und „stop sharing“ wählt) oder indem die Datei aus „my shared folders“ löscht, wird die dbb-Datenbank dahingehend geändert, dass diese Datei nicht freigegeben ist und der Zeitpunkt, wann KaZaA dieses Ereignis registriert hat, wird in der Datenbank festgehalten.

Wenn ein Datei aus einen freigegebenen Ordner gelöscht wird, kann der Eintrag über die betreffende Datei noch für eine lange Zeit in der dbb-Datenbank existieren.

Downloads

Wenn KaZaA einen Download beginnt, wird eine temporäre Datei in „my shared folders“ oder dem standardmäßig eingestellten Download-Ordner angelegt. Diese Datei wird mit downloadxxxxxxxxxxxxxxxxxx.dat benannt, wobei die „x“ 18 Ziffern repräsentieren.

Diese Datei besteht aus zwei unterschiedlichen Teilen. Der Dateianfang enthält Teile der gerade heruntergeladenen Datei, gefolgt von einem KaZaA-spezifischen „Nachspann“, der Informationen darüber enthält, von wo die Datei heruntergeladen wurde, z.B. IP-Adresse, Zeitpunkt und Benutzer-ID. KaZaA benutzt diese Informationen bei der Wiederaufnahme eines abgebrochenene Downloads.

Die Registrierdatenbank

Weitere Benutzerinformationen von Bedeutung werden in der Registry gespeichert. Dies umfasst den Benutzernamen, ob die Dateifreigabe auf Anwendungsebene ein- oder ausgeschaltet ist, und für die KaZaA Media Desktop Version 2 und höher, die letzten 50 Suchbegriffe in verschlüsselter Form.

Fragen & Antworten / Wie kann ich beweisen…

Der Beschuldigte behauptet, dass er nicht explizit nach Kinderpornografie gesucht hat, wie kann ich dieses Argument widerlegen?

Falls es sich bei der Clientsoftware um KaZaA Media Desktop Version 2 und höher handelt, exportieren Sie die Registry-Dateien und importieren Sie diese in KaZAlyser. Schauen Sie unter dem Registryschlüssel [HKEY_CURRENT_USER\Software\KaZaA\Search]. KaZAlyser zeigt die Liste der letzten 50 Suchbegriffe auf diesem Computer. Beachten Sie, dass diese Einträge in verschlüsselter Form in der Registry gespeichert sind; KaZAlyser entschlüsselt diese und zeigt sie im Klartext an.

Der Beschuldigte behauptet, dass er – nachdem er eine Site mit harmlosem Material gefunden hat, das ihn interessiert – die Option „finde alles von diesem Benutzer“ gewählt hat, ohne darauf zu achten, was im einzelnen heruntergeladen wurde.

1. Laden Sie die KaZaA-Datenbank-Dateien in KaZAlyser und laden Sie auch die Zeitstempel der Dateien. Es werden die Inhalte der KaZaA-Datenbank und die Zeitstempel der eigentlichen Dateien angezeigt. Wenn ein Download für mehrere Dateien beginnt, legt KaZaA einen temporären Platzhalter für jede Datei an, die gedownloaded werden soll (dies ermöglicht KaZaA, abgebrochene Downloads wieder aufzunehmen). Diese Dateien werden zum exakt gleichen Zeitpunkt angelegt (+/- wenige Millisekunden). Falls die Behauptung wahr ist, haben alle Dateien, deren Download zum gleichen Zeitpunkt gestartet wurde, denselben Zeitstempel.

2. KaZaA erstellt den temporären Dateinamen in der Form download12343223332223.dat, wobei die ersten Zahlen in codierter Form Datum und Uhrzeit des Downloads darstellen. Diese Dateien werden in den tatsächlichen Namen umbenannt, nachdem der Download erfolgreich abgeschlossen wurde.

   Wenn ein Download läuft, zeichnet KaZaA am Ende jeder temporären Datei verschiedene Daten auf, die die Downloadquelle(n) betreffen. Diese Information befindet sich in der temporären Datei. Verwenden Sie KaZAlyser, um temporäre Dateien zu laden und die Quellinformationen anzuzeigen. Wenn zu vermuten ist, dass mehrere Dateien von demselben Benutzer heruntergeladen wurden, dann erscheint sein Name und die IP-Adresse, die er zum Zeitpunkt des Downloads hatte, in jeder temporären Datei von ihm/ihr.

3. Wenn ein Download erfolgreich abgeschlossen ist, wird die temporäre Datei in den tatsächlichen Namen der Datei umbenannt. Wenn dies passiert, hinterlässt KaZaA oftmals einige Informationen in Bezug auf die Downloadquelle im „slack space“ am Ende der Datei. KaZAlyser versucht, diese Informationen zu entschlüsseln und in einer für Menschen lesbaren Form anzuzeigen.

   Leider scheint diese Information oft teilweise überschrieben zu sein, so dass nicht alle Daten verfügbar sind. Diese Information wird in komplexer Form gespeichert. Wenn Daten vorhanden sind und erfolgreich entschlüsselt werden können, kann man in einem sehr hohen Maß auf die Authentizität vertrauen.

Der Benutzer hat mehr als 5000 Dateien in seiner Datenbank, ich möchte nur Kinderpornografie identifizieren, wie kann ich dies tun?

Es gibt zwei Methoden:

1. den Filter „bekannte Kinderpornografie“ aus dem Filter-Menü verwenden. Dies durchsucht die Datenbank und zeigt nur solche Dateien an, die einen Hashwert besitzen, der zu einem aus der KaZAlyser-Datenbank bekannter Kinderpornografie passt.

2. alternativ verwenden Sie den Filter „möglicherweise Kinderpornografie“. Dieser Filter zeigt nur die Dateien an, die **scheinen** Kinderpornografie zu sein, basierend auf Schlüsselwörtern im Dateinamen, der Beschreibung, Schlagworten, Titel, Album oder Künstler.

Jede Methode hat ihre Vor- und Nachteile; während der erste Filter sehr wenige oder keine Falschalarme ausgibt, erkennt er keine Kinderpornografie, für die kein in der Hashwert-Datenbank existiert. Der Filter „möglicherweise Kinderpornografie“ wird wahrscheinlich mehr finden, aber auch eine große Zahl von Falschalarmen liefern. Versuchen Sie beide Methoden, weil sie wenig Zeit für einen Durchlauf benötigen und wählen Sie den Filter der am besten passt. Hinweis: Es ist dem Ermittler vorbehalten zu bestätigen, dass irgendein Material, das von KaZAlyser als Kinderpornografie identifiziert wurde, tatsächlich Kinderpornografie ist.

Ich möchte feststellen, von wo der Benutzer Dateien heruntergeladen hat

Hier ist an einige Bereiche zu denken. Zunächst extrahieren Sie den Inhalt eines freigegebenen Ordners in einen Arbeitsordner. Falls Sie Encase benutzen, benutzen Sie die „physical file“-Option, der die Datei und vorhandener „slack space“ am Ende der Datei extrahiert. Wählen Sie „File|Identify source of download“ aus dem Menü und wählen den o.g. Ordner.

Für jede teilweise heruntergeladene Datei gibt es einen oder mehrere Einträge (Zeilen), die Informationen enthalten, welche näher betrachtet werden müssen. Der Ermittler muss die gelisteten Remote-IP-Adressen in Verbindung mit den verschiedenen Zeitstempeln untersuchen, um festzustellen, ob die Remote-IP eine vielversprechende Adresse ist.

FASTTRACK PEER-TO-PEER NETZWERKSOFTWARE

Historie des Peer-to-Peer-Systems

Alle Peer-to-Peer File-Sharing-Systeme im Internet wurden entworfen, den Benutzern von PCs mit Internetzugang zu ermöglichen, Dateien direkt untereinander zu tauschen. Eines der ersten System war Napster, das zum Tauschen von Musikdateien konzipiert war, üblicherweise im MP3-Format. Napster wurde geschlossen, weil richterlich entschieden wurde, dass es ein System ist, das anderen erlaubt, gegen Copyright und geltendes Recht zu verstoßen. Die Schließung wurde durch die Tatsache erleichtert, dass Napster eine zentralen Computer benutzte, der alle gemeinsamen Dateien seiner Mitglieder auflistete. Es wurde deshalb argumentiert, dass Napster wusste, was und von wem getauscht wurde und die Napster-Organisation hatte die Kontrolle über Copyrightverletzungen etc.

In der Folgezeit nahmen vier andere Peer-to-Peer Netzwerksysteme – ursprünglich alle in erster Linie auf den Tausch von Musikdateien ausgelegt – den Betrieb auf. Sie benutzten alle dieselbe Arbeitsmethode und dieselbe Software. Die Software wurde (und wird) FastTrack genannt, und die vier Organisationen, die sie benutzten, wurden unter den Namen Morpheus, KaZaA, Grokster und FileShare bekannt.

Aufgrund der Art, wie diese Organisationen strukturiert sind, wurden sie noch nicht gerichtlich belangt, obwohl ein Verfahren rechtshängig ist. Der Unterschied in der Struktur wird später in Teil 2 erläutert.

Anfang 2002 kam es zu Rechtsstreitigkeiten in Bezug auf die Lizenzierung der FastTrack-Clientsoftware zwischen FastTrack und dem Morpheus-System. Diese hatten zum Ergebnis, dass die Morpheus (Music City) Organisation zu einer anderen, nicht kompatiblen Clientsoftware namens Gnutella (genauer Gnucleus), wechselte und dadurch von den anderen drei Organisationen „wegbrachen“.

Die FastTrack-Struktur

Anstatt eines zentralen Verzeichnisses der verfügbaren Dateien (wie es Napster tat) arbeitet die FastTrack-Software auf der Basis einer großen Zahl von „Superknoten“ (supernodes), die über die ganze Welt verteilt sind.

Jeder Superknoten enthält ein suchbares Dateiverzeichnis, das auf den FastTrack-Clients verfügbar ist, die gerade mit ihm verbunden sind. Wenn sich ein neuer Client mit dem Internet verbindet, und dann mit dem FastTrack-System, wird er einem Superknoten zugewiesen. Von nun an werden alle von diesem Client angebotenen Dateien auf dem Superknoten gelistet und stehen für andere zum Download zur Verfügung.

Auf diese Weise sind die FastTrack-Organisationen, KaZaA, Grokster und FileShare in der Lage zu behaupten, dass keine Kenntnis davon haben, welche Dateien auf dem System getauscht werden, da sie die Superknoten nicht unter Kontrolle haben und sie deshalb nicht denselben rechtlichen Verpflichtungen wie Napster unterliegen.

Anschluss an eines der Peer-to-Peer Systeme

Um sich einem der FastTrack Peer-to-Peer-System anzuschließen, muss sich ein Internet-Benutzer zunächst eine Kopie der FastTrack-Clientsoftware besorgen. Diese ist als frei verfügbarer Download über einige Sites im World Wide Web verfügbar, oder sie kann gekauft werden. Die meisten Benutzer laden die kostenlose Version aus dem Web herunter.

Anschließend muss der Internetbenutzer die Software zunächst auf seinem/ihrem Computer installieren. Das Programm stellt am Ende des Installationsprozesses eine Internetverbindung zu einem Zentralcomputer her, der die Benutzernamen verwaltet.

Der Benutzer wird aufgefordert, einen Benutzernamen zu wählen, der innerhalb des FastTrack-System verwendet wird. Dieser Name muss in keinerlei Bezug zu dem realen Namen des Benutzers oder seiner E-Mail-Adresse stehen, obwohl dies möglich ist. So *könnte* ein Benutzer mit dem Namen Fred Smith den Benutzername FredSmith, oder sagen wir, Freddie wählen, aber es kann gut der Fall sein, dass der eine zufällige Reihe von Buchstaben wählt, wie djdjdjdjdj.

Die FastTrack-Software des Benutzers „merkt" sich diesen Benutzernamen nachdem er gewählt und registriert wurde, und verwendet ihn ab diesem Zeitpunkt automatisch, wann immer die FastTrack-Software aufgerufen wird.

Nichts davon bringt eine finanzielle Gebühr für den Benutzer mit sich (es sei denn, er/sie entschließt sich dazu, die FastTrack-Software zu kaufen).

Software und Datenstruktur auf dem Computer eines Mitglieds

Nehmen wir die KaZaA FastTrack-Software als Beispiel, wird sich der Benutzer typischerweise die Software über einen Link auf der KaZaA-Webseite http://www.kazaa.com herunterladen. Der Installationsprozess installiert die Software, standardmäßig unter C:\Programme\KaZaA auf dem Computer des Benutzers.

Weiterhin werden zwei wichtige Unterverzeichnisse oder Ordner an dieser Stelle angelegt. Eines davon heißt „DB" und enthält Datenbank-Dateien, die die Datei-Freigabe auf dem Rechner des Benutzers verwalten und ein anderer Ordner heißt „My Shared Files".

In der Standardeinstellung wird jede Datei, die der Benutzer in „My Shared Files" ablegt, für andere FastTrack-Benutzer verfügbar gemacht, wenn der Benutzer online ist – d.h., verbunden mit dem Internet und laufender FastTrack-Software.

Darüber hinaus werden Dateien, die der Benutzer von anderen FastTrack-Clients herunterlädt, standardmäßig in den Ordner „My Shared Files" abgelegt und sind auch automatisch für andere Benutzer verfügbar, sobald der Download auf der Benutzermaschine abgeschlossen ist (aber nicht vorher).

Zusätzlich ermöglicht es die FastTrack-Software dem Benutzer, andere Dateien, Ordner oder sogar ganze Laufwerke auf seinem/ihrem Computer zum Tausch über das Peer-to-Peer-Netzwerk verfügbar zu machen.

FastTrack Suchfunktionen

Die FastTrack-Clientsoftware hat eine Reihe verschiedener Bildschirmmasken, die der Benutzer für verschiedene Zwecke einsetzen kann. Einer der wichtigsten ist eindeutig die Suchmaske.



Nach dem Öffnen der Suchmaske kann der Benutzer angeben, nach welchem Dateityp er/sie sucht. Die Auswahl sind Video, Audio, Software, Bilder oder Dokumente. Alternativ kann sich der Benutzer zu einer Suche über alle Typen entscheiden, indem er die „Everything“-Option verwendet.

Ein Suchbegriff wird im „Search for:“-Feld eingegeben, und die „Search Now“-Schaltfläche wird angeklickt. Der Superknoten, mit dem der Benutzer verbunden ist, wird dann nach Dateien durchsucht, die zu dem Suchbegriff des Benutzers passen.

Der Benutzer kann die maximale Trefferzahl bis zu 200 festlegen. Das Suchergebnis wird rechts neben dem Suchfeld angezeigt.



Die hier gezeigte Suche war in der Audio-File-Kategorie und verwendete den Suchbegriff „spears“ als Künstlernamen. Ein Teil des Suchergebnisses wird hier rechts vom Suchfeld anzeigt.
Wenn ein kleines Pluszeichen neben dem Eintrag angezeigt wird, bedeutet dies, dass mehr als ein Benutzer auf diesem Superknoten dieselbe Datei zum Download anbietet. Die Musikdatei „Lucky“ wird daher so angeboten, aber nur ein Benutzer bietet „Girl in My Mirror“ an.

Für den Benutzer verfügbare Datei-Information

Die Information für jeden in der Suchmaske angebotenen „Treffer“ sind folgende:

- Eine Beschreibung des Eintrags (dies ist ein Alias, nicht der tatsächliche Dateiname)
- Der Künstler
- Das Album (für Musikdateien)
- Die Kategorie (für Musik Pop, Klassik etc.)
- Die ETA (Estimated download time – geschätzte Downloadzeit)
- Der/die Benutzer, welche die Datei anbieten
- Die Qualität der Aufnahme (sampling rate)
- Die Spielzeit in Stunden, Minuten und Sekunden
- Die Dateigröße in Kilobyte
- Die geschätzte Bandbreite, die dem anbietenden Benutzer zur Verfügung steht

- Der tatsächliche Dateiname, einschließlich der Dateierweiterung, die das Dateiformat anzeigt, z.B. .mpg oder .avi.



Die Information ist ähnlich für Videodateien, mit der Ausnahme, dass Album fehlt und die Spalten „Type“ und „Language“ vorhanden sind.

Zusätzlich werden oftmals weitere Informationen angezeigt, wenn mit dem Mauszeiger über ein Eintrag gefahren wird, wobei manche Daten der Bildschirmmaske wiederholt werden. Auf der Abbildung kann erkannt werden, dass es sich bei der betreffenden Datei um eine Videodatei handelt, die von einem Benutzer names vincentengel@KaZaA angeboten wird, dass die Dateigröße 4.896 KB beträgt, dass die Spielzeit 22 Sekunden und der tatsächliche Dateiname Britney Spears lautet – HBO Commerical.mpeg.

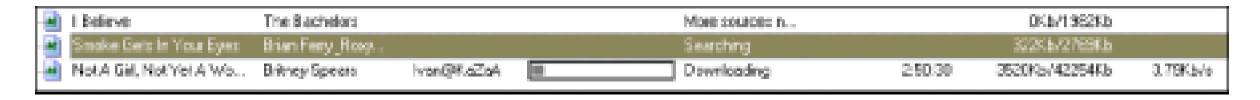
Innerhalb der Suchmaske hat der Benutzer auch die Möglichkeit, durch Rechtsklick auf einen „Treffer“ eine Liste aller Dateien des Benutzers anzufordern, der ausgewählte Datei anbietet. Dies ist ein wichtiges Werkzeug für den Ermittler, das ihn in die Lage versetzt, eine vollständige Liste aller Dateien zu erhalten, die ein ausgewählter Benutzer zum Tausch anbietet.

Herunterladen einer Datei

Um eine Datei herunterzuladen, ist es für den Benutzer nur notwendig, entweder einen Rechtsklick auf die gewählte Datei auszuführen und dann „Download“ auszuwählen, oder alternativ aus die gewählte Datei doppelzuklicken. Jede dieser Aktionen startet den Download auf die Maschine des Benutzers.

Falls ein Benutzer den Download von Dateien in einem Peer-to-Peer-Netzwerk überwachen möchte, kann er dies durch Umschalten auf die „Traffic“-Bildschirmmaske tun. Es ist möglich, viele verschiedene Dateien gleichzeitig herunterzuladen, und der Fortschritt jeder einzelnen Datei wird der „Traffic“-Bildschirmmaske angezeigt.

Diese Bildschirmmaske hat zwei Teile. Der obere Teil zeigt die Details jedes laufenden Downloads auf die Benutzermaschine, und der untere Teil zeigt die Details jedes laufenden Uploads von der Benutzermaschine (vgl. folgenden Bildschirm).



Die obige Abbildung zeigt einen Ausschnitt des Downloadfensters. Eine Datei mit Namen „Not a Girl, Not Yet a Wo(man)’ von Britney Spears wird gerade dem Benutzer Ivan@KaZaA heruntergeladen. 3520 KB von insgesamt 42.254 KB wurden bereits heruntergeladen, und bei der aktuellen Geschwindigkeit schätzt das System, dass der Download in 2 Stunden, 50 Minuten und 30 Sekunden abgeschlossen sein wird. Die Transfergeschwindigkeit beträgt 3,79 Kilobits pro Sekunde (Kb/s). Über dieser Zeile sucht das System nach einer Kopie eines Musikstücks von Brian Ferry, und darüber befindet sich eine andere Downloadanforderung, die eingestellt wurde, weil gerade kein Benutzer online ist, der diese Datei anbietet. Entweder wurde sie in

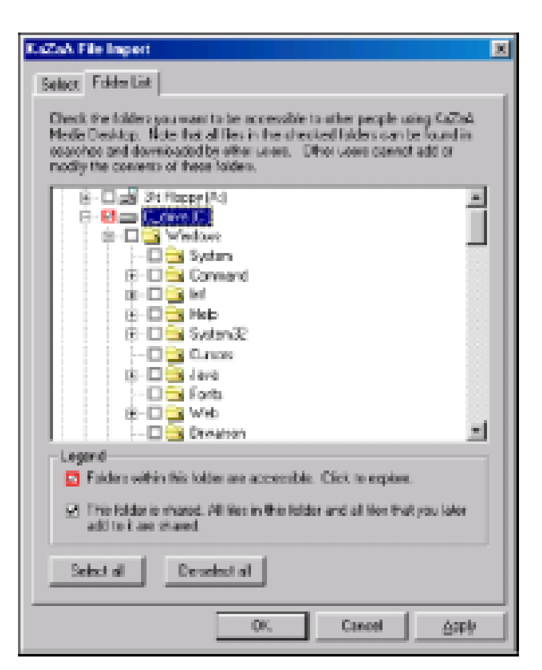
einer früheren Sitzung ausgewählt, als sie angeboten wurde, oder Benutzer, der sie angeboten hat ging offline oder sein System in zu sehr ausgelastet, um die Datei liefern zu können.

Falls mehr als eine Benutzer eine bestimmte Datei anbietet, kann ein „segmentierter Download“ stattfinden. Ein segmentierter Download liegt vor, wenn verschiedene Teile der angeforderten Datei von verschiedenen Benutzern im Netzwerk zu Verfügung gestellt werden. Dies beschleunigt den Downloadprozess, und bedeutet, dass der anfordernde Benutzer nicht von einem einzelnen Benutzer abhängig ist. Benutzer im System können kommen und gehen, aber der Download wird fortgesetzt.

Wie bereits erwähnt wird die heruntergeladene Datei standardmäßig im Ordner „My Shared Files“ gespeichert, und sobald der Download abgeschlossen ist, ist sie in der Standardeinstellung für andere Peer-to-Peer Netzwerkbenutzer zum Tausch verfügbar, obwohl diese durch den herunterladenden Benutzer verhindert werden kann.

Wie in der Suchen-Bildschirmmaske existiert die Möglichkeit für den Benutzer, eine Dateiliste abzurufen, die von einem bestimmten Benutzer angeboten wird. So kann in dem oben geschilderten Fall der Benutzer durch einen Rechtsklick die Liste von Ivan@KaZaA abrufen, von dem er die Britney Spears-Datei heruntergeladen hat. Dadurch wechselt die Ansicht zu der Suchen-Bildschirmmaske und die Ergebnisse werden angezeigt.

Dateien mit andere Benutzern teilen



Der Benutzer eines Clientcomputers hat die vollständige Kontrolle, welche Dateien im Netzwerk freigegeben sind und welche nicht. Der Benutzer könnte sich entscheiden, keinerlei Dateien freizugeben, oder nur einige Dateien in „My Shared Files“ oder alle in diesem Ordner oder Dateien in anderen Ordnern oder andere Laufwerken des Clientcomputers freizugeben. Die Abbildung rechts zeigt das Werkzeug, mit dem weitere Daten auf dem Rechner zur Freigabe bestimmt werden können.

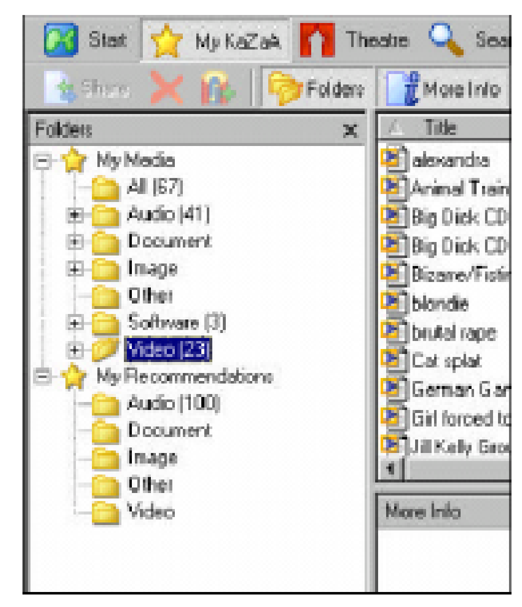
Der Benutzer ist sich zu jedem Zeitpunkt im Klaren, was freigegeben ist, da diese Information kontinuierlich am unteren Rand des FastTrack-Bildschirms angezeigt und aktualisiert wird (egal welcher aktiv ist). Falls der Benutzer keinerlei Dateien freigegeben hat, ist dies in der Fußleiste klar ersichtlich, wie in der Abbildung unten.

,898,746 users online, sharing 317,737,008 files (2,367,104 GB) | Not sharing any files

Falls der Benutzer Dateien freigegeben hat, dann wird die Tatsache, dass dies passiert, wieder klargemacht. Im nächsten Beispiel hat der Benutzer 50 Dateien freigegeben.



Unter diesen Umständen ist es vermutlich schwierig für den Beschuldigten abzustreiten, dass er/sie sich bewusst war, dass auf seinem/ihrem Computer Dateien für andere Benutzer verfügbar waren.



Darüber hinaus gibt es eine andere Bildschirmmaske im FastTrack-Client mit dem Namen „My KaZaA“ (oder entsprechend für Grokster und FileShare), die Details über die Dateien zeigt, die auf dem Benutzercomputer freigegeben sind, egal wo sich diese auf der Maschine befinden. Diese Maske ist nach Dateitypen unterteilt, und zeigt durch verschiedene Icons für jede Datei grafisch an, welche gerade freigegeben ist und welche nicht. In der Beispielabbildung rechts hat der Benutzer 67 Dateien freigegeben, davon sind 41 Musikdateien, 3 Software- und 23 Videodateien. Das Videoverzeichnis ist geöffnet und zeigt die Details für diese Dateien.

Uploads überwachen und kontrollieren

Falls Dateien auf dem Benutzerrechner zum Tausch vorhanden sind, und die Freigabe eingeschaltet ist, ist es wahrscheinlich, dass Uploads von dieser Maschine stattfinden.

Wenn dies passiert, werden Details dieser Uploads in der unteren Hälfte der „Traffic“-Bildschirmmaske in der gleichen Weise angezeigt, wie Downloads im der oberen Hälfte (siehe oben). Sogar wenn der Upload abgeschlossen ist, wird die Tatsache, dass dies passiert ist, weiterhin in der unteren Hälfte der „Traffic“-Bildschirmmaske angezeigt. So werden nicht nur gerade laufende Uploads angezeigt, sondern auch solche, die während der Peer-to-Peer Sitzung stattgefunden haben. Das Fenster wird gelöscht, wenn sich entweder der Benutzer dazu entscheidet, oder die FastTrack-Software beendet wird.

Nochmals, diese Anzeige zeigt dem Benutzer des Rechners Details aller Uploads, die von seinem/ihrem Computer stattgefunden haben, klar und deutlich an. Während eines Uploads wird sogar der Name des Clients angezeigt, der den Upload vornimmt.

Der Benutzer kann laufende Uploads abbrechen, wenn er/sie dies wünscht und kann in der FastTrack-Software auch angeben, wie viel gleichzeitige Uploads von seiner/ihrer Maschine zugelassen sind sowie die zugelassene Bandbreite für Uploads. Mit anderen Worten, der Benutzer hat volles Bewusstsein und Kontrolle über die Upload-Aktivitäten von seinem Computer.

IP-Adressen und die Bedeutung der Zeit

Wann immer ein Computer mit dem Internet verbunden wird, wird ein Merkmal festgelegt, *das zu einem bestimmten Zeitpunkt für diese Maschine im Internet eindeutig ist*. Dieses Merkmal wird IP- (Internet Protocol) Adresse genannt und wird in Form einer Serie von vier Zahlen dargestellt, die durch drei Punkte getrennt sind. Ein Beispiel könnte 151.32.205.199 sein.

Jede Zahl muss im Bereich 0 bis 255 liegen.

Jedem Internet Service Provide (ISP) ist ein Bereich von IP-Adressen zur Kundennutzung zugeteilt. So hat z.B. die British Telecom einen Bereich, NTL einen anderen usw. Wann immer einer ihrer Benutzer eine Internetverbindung herstellt, weist der ISP diesem eine IP-Adresse für die Dauer der Sitzung zu. Wenn ein Benutzer die Verbindung beendet, kann die IP-Adresse sehr wohl einem anderen Benutzer zugewiesen werden, aber eine IP-Adresse kann niemals gleichzeitig an mehr als einen Benutzer vergeben sein. Das Internet lässt dies einfach nicht zu.

ISP's protokollieren diese IP-Adressen-Vergaben (für eine begrenzte Zeit) und können sie auf Anfrage feststellen, um Strafverfolgungsbehörden bei der Aufklärung krimineller Aktivitäten unterstützen, vorausgesetzt, dass ein Rechtsersuchen vorliegt.

Folglich kann – wenn die IP-Adresse eines Computers zusammen mit der exakten Datums- und Zeitangabe ermittelt wird – die Kombination dieser Elemente einen Computer im Internet eindeutig identifizieren. Der ISP kann Namen und Adresse dieser Person und oft weitere Informationen zur Verfügung stellen.